UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,910	02/21/2002	Laszlo Hars	US 020051	3945

24737	7590	12/21/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER
DO, CHAT C

ART UNIT	PAPER NUMBER
2124	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE **3** MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *2/21/02; 4/18/02; 9/24/03.*

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-25* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-5, 7-13, 15-23, 25* is/are rejected.

7) ☒ Claim(s) *6,14 and 24* is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *9/24/03.*

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2.   Claims 5, 7, 13, 15, 19-20, 23, and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Re claim 5, the parameter "n" in line 4 lacks antecedence basis. The applicant does not define what's exactly the "n" parameter. For examination purposes, the examiner considers n as any integer value. Claims 13, 19, and 23 have the same rejection.

Thus, claims 7, 15, 20, and 25 are also rejected for being dependent on the rejected base claims 5, 13, 19, and 23 respectively.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.　　　Claims 1-4, 8-12, 16-18, and 21-22 are rejected under 35 U.S.C. 103(a) as being obvious

over Brennan et al. (U.S. 5,675,649) in view of NIST ("Random Number Generation and

Testing").

Re claim 1, Brennan et al. disclose in Figure 2 a method for testing randomness

when generating a random number (abstract and Figure 2 wherein the test is doen in step

or process 30-34), the method comprising the steps of: generating (output of 30) random

sequences of binary bits; applying (input into the test in 32) generated random sequences

to a test at a predefined block interval of k bits at a time to compute an average number of

occurrences for each predefined block; and, determining (e.g. 34) whether generated

random sequences are sufficiently random by comparing the output of exponential

overlapping count operation A to a predetermined acceptance range. Brennan et al. do

not disclose the test is an exponential overlapping count operation A. However, NIST

discloses in pages 2-3 an exponential overlapping count operation A (e.g. overlapping or

periodic template matching test). Therefore, it would have been obvious to a person

having ordinary skill in the art at the time the invention is made to add the test as an

exponential overlapping count operation as seen in NIST's invention into Brennan et al.'s

invention because it would enable to simplify to determine the randomness of a random

sequence to increase the system performance.

Re claim 2, Brennan et al. further disclose in Figure 2 the step of determining that

generated sequences are sufficiently random when the output of exponential overlapping

count operation A falls between predetermined acceptance range (e.g. col. 22 lines 35-43

wherein the number of time is one).

Re claim 3, Brennan et al. in view of NIST do not disclose in Figure 2 the step of notifying that generated random sequences are not sufficiently random when the output of exponential count operation A falls outside of predetermined acceptance range. However, Brennan et al. mentioned about the trust between the user and the generation of randomness (page 1 lines 38-44) that the user would like to know the whole operations in order to truly trust. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a step of notifying the user if the generated random bits are not sufficiently random as suggested in the drawback of background of the invention into Brennan et al. in view of NIST's invention because it would enable to enhance the system's flexibility by alerting the operator to aware the insufficient random bits.

Re claim 4, Brennan et al. further disclose in Figure 2 the step of generating a new set of random sequences when the output of exponential count operation A falls outside of predetermined acceptance range (e.g. loopback into the random generator sequence 30 if it fails or fall outside the predetermined acceptance range in Figure 2).

Re claim 8, it has same limitations cited in claim 3. Thus, claim 8 is also rejected under the same rationale as cited in the rejection of rejected claim 3.

Re claim 9, Brennan et al. further disclose in Figure 2 the step of: repeating said steps (a) - (c) until any of the computed exponential averaging value falls outside of predetermined acceptance range (e.g. looping Figure 2 for every time to generate a new random bits).

Re claim 10, it has same limitations cited in claim 3. Thus, claim 10 is also rejected under the same rationale as cited in the rejection of rejected claim 3.

Re claim 11, it has same limitations cited in claim 4. Thus, claim 11 is also rejected under the same rationale as cited in the rejection of rejected claim 4.

Re claim 12, Brennan et al. further disclose in Figure 2 random number generator is embedded in a smart card (Figure 2).

Re claim 16, it is an apparatus claim of claim 1. Thus, claim 16 is also rejected under the same rationale as cited in the rejection of rejected claim 1.

Re claim 17, it is an apparatus claim of claim 2. Thus, claim 17 is also rejected under the same rationale as cited in the rejection of rejected claim 2.

Re claim 18, it is an apparatus claim of claim 3. Thus, claim 18 is also rejected under the same rationale as cited in the rejection of rejected claim 3.

Re claim 21, it is an instruction claim of claim 1. Thus, claim 21 is also rejected under the same rationale as cited in the rejection of rejected claim 1.

Re claim 22, it is an instruction claim of claim 3. Thus, claim 22 is also rejected under the same rationale as cited in the rejection of rejected claim 3.

Allowable Subject Matter

5.   Claims 5, 7, 13, 15, 19-20, 23, and 25 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

6.   Claims 6, 14, and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

    a.   U.S. Patent No. 6,675,113 to Hars discloses a monobit-run frequency on-line randomness test.

    b.   U.S. Patent No. 6,215,874 to Borza et al. disclose a random number generator and method for same.

    Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (571) 272-3721. The examiner can normally be reached on M => F from 7:00 AM to 5:30 PM.

    If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (571) 272-3719. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do
Examiner
Art Unit 2124

November 30, 2004

TODD INGBERG
PRIMARY EXAMINER